

**CYSE 280 - Windows Systems Management and Security**

**Professor Malik A. Gladden**

**Homework 12**

**Short Answer Questions** (short answers should generally be at least three to four sentences in length. However, it is important to be as concise as possible when responding.) or you may choose to **Upload a Two-Minute Audio or Video recording** to answer the following questions.

## **Modules 9 & 10**

### **1. Why is the main purpose of using Secure Socket Layer (SSL)?**

SSL (Secure Socket Layer) encrypts data between a client and server to prevent unwanted access and guarantee secure internet communication. It also offers authentication by employing SSL certificates from credible Certificate Authorities to confirm the identity of the client and server. In addition, SSL protects data integrity by identifying illegal changes made while in transit. Its function is unchanged even though Transport Layer Security (TLS) has now taken its place.

### **2. What are the advantages and disadvantages of using Trusted Platform Module (TPM)?**

A hardware-based security component called the Trusted Platform Module (TPM) provides increased security by keeping critical information, including cryptographic keys, safe. It is compatible with Digital Rights Management (DRM), secure boot, protection against physical threats, hardware-based encryption, and platform integrity verification. However, it can be expensive, complicated, hardware-dependent, and have limited compatibility with older devices. Also, it may limit user freedom, cause vendor lock-in, and raise privacy issues. Despite these limitations, TPM is a useful tool for both users and businesses since it provides strong security advantages for data protection, secure boot, and encryption.

**Listen to “Episode #21: Black Duck Eggs Diaries podcast which can be found at**

**<https://darknetdiaries.com/episode/21/>**

**Based on the podcast, answer the following questions.**

- 1. How did law enforcement authorities manage to trace the illegal activities back to the main suspect in the case?**

When Ira and his group discovered the pseudo-Chinese business, the FBI was able to connect it to the illegal activities of the Chinese threat actors. Ira discovered this site while conducting an OSINT investigation on the Global 5 group after seeing a fake second headquarters location online. The "special menu item" that a worker who worked at the pseudo-Chinese restaurant had asked Ira to sample turned out to be a code for something else. Ira came to this conclusion after working as an NSA intelligence officer.

- 2. What was the significance of the term "Black Duck Eggs" in the context of the episode's story?**

The phrase "black duck eggs" describes Ira's discovery of a fake Chinese restaurant near the Global 5 company's headquarters. The goal of this fake Chinese restaurant was to find people who would help the Chinese government steal assets and trade secrets from the Global 5 corporation. You would have to request black duck eggs from the "special menu" to get accepted as a spy by the pseudo-Chinese restaurant, which would automatically start an interview.

### References

*Black Duck Eggs – Darknet Diaries*. (n.d.). <https://darknetdiaries.com/episode/21/>